

Nordic Cyber for Healthcare Forum by DNV

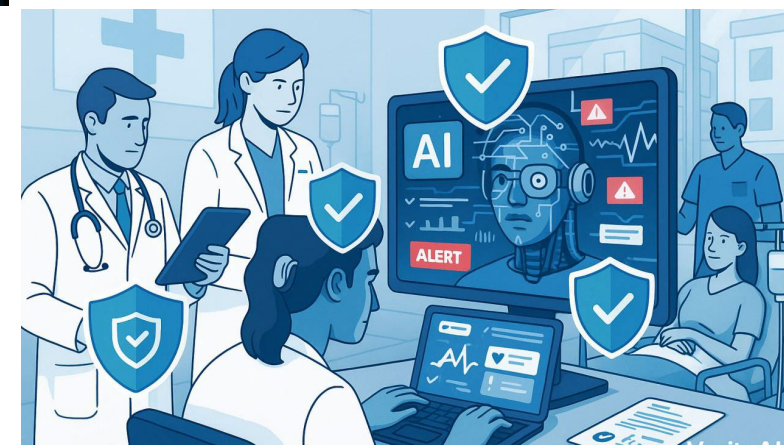
Morten Thorkildsen
Project Lead



As AI accelerates in healthcare, are we ready to govern it?



AI adoption and risk management survey





Findings from the AI adoption and risk management survey

August–September 2026

The story in one line

AI is moving into core healthcare workflows faster than governance and assurance are maturing.

5

Nordic countries

represented through the forum network

12

survey responses

from large and complex Nordic healthcare organisations



Three key messages

1

AI is moving from pilots to core treatment

2

Governance is not yet consistent

3

Risk management must become lifecycle-based

The opportunity is significant, but safe adoption requires enterprise governance and continuous monitoring



Why this survey matters

Nordic healthcare leaders are moving into a new phase of AI adoption: from experimentation to governed clinical and operational deployment.

Forum role

The Nordic Cyber for Healthcare Forum connects healthcare risk management and security leaders across the Nordic region to share experience and prepare for common cybersecurity challenges.

Survey purpose

The survey was prepared for the 6th Nordic Cyber for Healthcare Forum in Brussels and Leuven and is intended to strengthen shared understanding of AI adoption in Nordic healthcare.

Shared Nordic learning

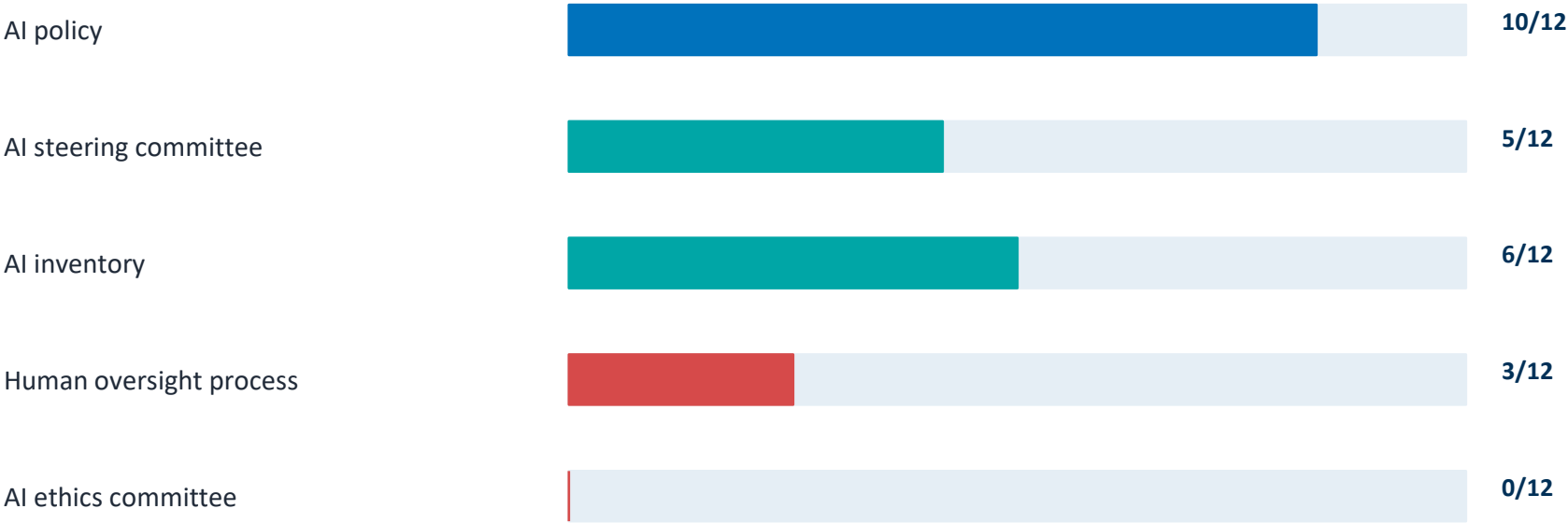


FINDING 1

Governance is emerging

Reported governance elements in place among 12 respondents

«Which of the following governance elements are established?»



Interpretation

AI is becoming a clinical, operational and strategic capability, but accountability has not yet consistently moved from individual AI projects to an enterprise-level governance model.



Two governance gaps stand out: boards and accountability

1 Board preparedness

«How prepared is your Board for AI-related decisions?»

Average preparedness for AI-related decisions is reported at 2.73 out of 5.

Key point: AI is becoming a board-relevant risk topic, not only a technology or innovation issue.

2.73 / 5

average board preparedness score

2 Accountability

«Who has overall accountability for AI governance?»

No common model for AI ownership has emerged across respondents.

Responsibility is reported across CEOs, CIOs, CMIOs, system owners, boards and EVP-level functions. Two respondents report no defined owner.

Needed: one clear executive owner and escalation path.

AI needs to be governed as a clinical, operational and strategic capability - with board awareness and clear ownership.



Adoption is strongest where value is visible and workflows are clear

«Which AI use cases are currently deployed?»



Investment focus next 2 years is also concentrated in ambient documentation, clinical decision support and radiology.

AI is already entering both administrative and clinical workflows - which makes governance, safety and cybersecurity a board-level issue.



FINDING 4

The perceived risk agenda is dominated by safety, privacy, trust and cyber risk

«Which AI risks are considered most significant? (Rank top five)»



Patient Safety gap

Patient safety is ranked with the highest perceived risk

Cybersecurity gap

The survey points to a need for more work to secure AI systems against cyber threats.



Supplier evidence and regulatory clarity are becoming critical

Vendor assurance

«How confident are you in the cybersecurity maturity of AI vendors?»

The survey indicates that more evidence from AI suppliers may be needed. This makes supplier cybersecurity, model governance, data handling and post-market monitoring central to procurement.



Regulatory readiness

«What is the biggest obstacle to secure AI deployment?»

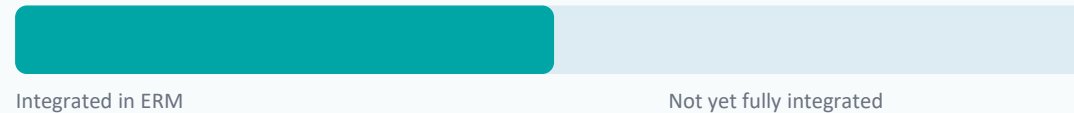
Regulatory uncertainty is reported as the biggest obstacle to secure AI adoption. Many organisations are still building the capability to translate regulatory requirements into clinical practice.

AI-specific risk assessment is only partly embedded in enterprise risk management

«Have AI-specific risk assessments been incorporated into your enterprise risk management process?»

Around half

have incorporated AI-specific risk assessments into ERM



What this signals

AI risk is moving from isolated project reviews into enterprise risk management — but the transition is incomplete and uneven across organisations.

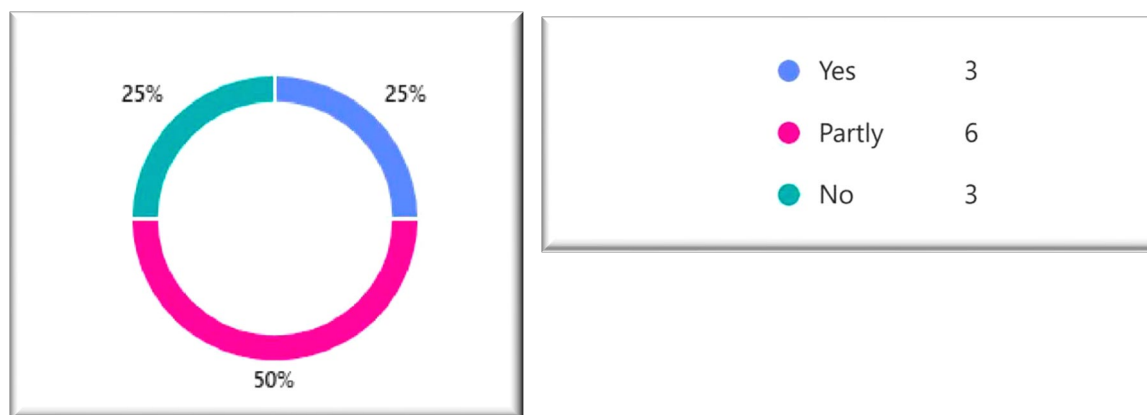
Why it matters

AI risk cuts across clinical safety, privacy, cybersecurity, suppliers and regulation. It needs shared ownership, escalation paths and lifecycle controls.

AI increasingly influences clinical workflows and decisions, but

...only 3 of 12 fully include AI in clinical safety assessments

«Are AI systems included in clinical safety assessments?»



WHAT THIS SIGNALS

Clinical safety governance for AI remains partial or fragmented in most organisations.

WHY IT MATTERS

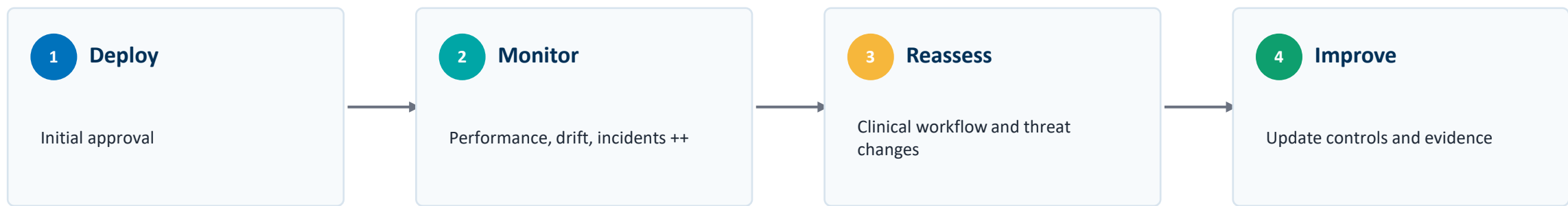
Patient safety, workflow integrity and accountability may go unmanaged

AI is entering clinical workflows faster than clinical safety assurance is being embedded.



AI risk management must continue after go-live

An AI system that was safe, secure and clinically effective when deployed may not remain so.



«How frequently are AI risks reassessed?»

9/12

perform AI risk reassessments ad hoc

Why this matters

Patient populations, workflows, models, suppliers, technology and cyber threats change after deployment.



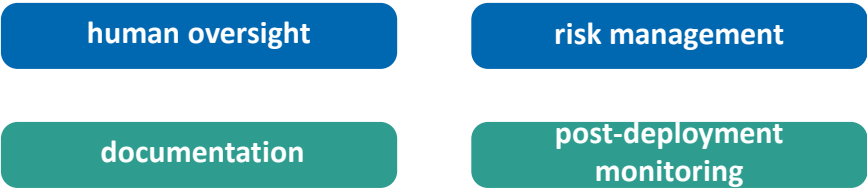
AI Act readiness: the gap is operational, not only legal

The survey indicates that Nordic healthcare organisations are preparing for the AI Act, but several practical controls are still unevenly implemented.

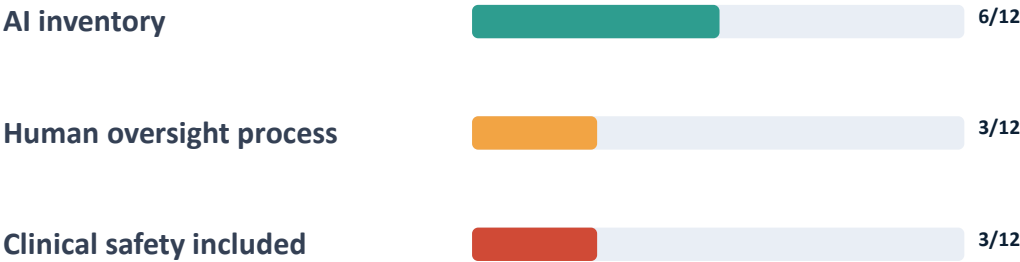
«How prepared is your organization for the EU AI Act?»

What the AI Act will require in practice

For high-risk healthcare AI, organisations will need stronger evidence that systems are governed, overseen, documented and monitored throughout their lifecycle.



What the survey suggests today



Many are still translating regulatory requirements into operational clinical practice.

AI Act readiness will depend on practical evidence - inventories, oversight, safety assessment, supplier assurance and lifecycle controls.